

1 George Haines
2 Nevada Bar No. 9411
3 Gerardo Avalos
4 Nevada Bar No. 15171
FREEDOM LAW FIRM
5 8985 S. Eastern Avenue Suite 100
6 Las Vegas, NV 89123
7 Telephone: 702-880-5554
8 Facsimile: 702-385-5518
9 Email: info@freedomlegalteam.com
10 *Counsel for Plaintiff and the Proposed Class*
11 *(additional counsel appear on signature page)*

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

KATHLEEN JORDAN, individually and on
behalf of all others similarly situated,

Plaintiff,
v.

ABSOLUTE DENTAL GROUP, LLC,

Defendant.

Case No. 2:25-cv-00986

CLASS ACTION COMPLAINT

Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff Kathleen Jordan (“Plaintiff”), individually and on behalf of all similarly situated persons, alleges the following against Absolute Dental Group, LLC (“ADG” or “Defendant”) based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation by Plaintiff’s counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against ADG for its failure to properly secure and safeguard Plaintiff's and other similarly situated ADG patients' personally identifiable information ("PII") and protected health information ("PHI"), from criminal hackers, including at least some of the following information, among other sensitive information: names, dates of birth, health information, dental information and records, doctor's name, health and/or dental insurance information, medical billing or claims information, prescription or medication information, Social Security numbers, and treatment information ("Private Information").

2. ADG is a Nevada-based dental care provider that serves many thousands of patients.

3. On or about May 2, 2025, ADG filed a notice with the United States Department of Health and Human Services Office for Civil Rights (HHS OCR), disclosing a data breach impacting ADG’s network servers (the “Data Breach”).¹

4. Little detail is available concerning the Data Breach and ADG has failed to disclose critical information about its investigation, post-breach containment, and remediation efforts that would enable breach victims to take necessary steps to protect themselves against the harms caused by the Data Breach.

¹ Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Department of Health and Human Services Office for Civil Rights https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 2, 2025)

1 5. Because of ADG's conduct and data privacy failures, Plaintiff and Class Members
2 are and continue to be at a significant risk of identity theft and various other forms of personal,
3 social, and financial harm. The risk will remain for their respective lifetimes.

4 6. The Private Information compromised in the Data Breach includes highly sensitive
5 data, which is a gold mine for data thieves. Armed with sensitive Private Information, data thieves
6 can commit a variety of crimes including, e.g., opening new financial accounts in Class Members'
7 names, taking out loans in Class Members' names, using Class Members' names to obtain medical
8 services, using Class Members' information to obtain government benefits, filing fraudulent tax
9 returns using Class Members' information, and giving false information to police during an arrest.

10 7. Despite reporting the Data Breach to HHS OCR, ADG has provided no assurance
11 that all personal data or copies of data have been recovered or destroyed, or that it has adequately
12 enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

13 8. Therefore, Plaintiff and Class Members have suffered and remain at an imminent,
14 immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm
15 from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit
16 of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data
17 Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the
18 Data Breach.

19 9. Plaintiff brings this class action lawsuit to address ADG's inadequate safeguarding
20 of Class Members' Private Information that it collected and maintained, and its failure to provide
21 timely and adequate notice to Plaintiff and Class Members of the types of information that were
22 accessed, and that such information was subject to unauthorized access by cybercriminals.

23 10. The potential for improper disclosure and theft of Plaintiff's and Class Members'
24 Private Information was a known risk to ADG, and thus ADG was on notice that failing to take
25 necessary steps to secure the Private Information left it vulnerable to an attack.

26 11. Upon information and belief, ADG failed to properly monitor and implement
27 security practices with regard to the computer network and systems that housed the Private
28 Information.

1 12. Plaintiff's and Class Members' identities are now at risk because of ADG's
 2 conduct, as the Private Information that ADG collected and maintained is now in the hands of data
 3 thieves and other unauthorized third parties.

4 13. Plaintiff seeks to remedy these harms on behalf of Plaintiff and all similarly situated
 5 individuals whose Private Information was accessed and/or compromised during the Data Breach.

6 14. Accordingly, Plaintiff, individually and on behalf of the Class, asserts claims for
 7 negligence, negligence per se, breach of express and implied contract, unjust enrichment, breach
 8 of fiduciary, breach of confidence, and declaratory and injunctive relief.

9 II. PARTIES

10 Plaintiff

11 *Plaintiff Kathleen Jordan*

12 15. Plaintiff Kathleen Jordan is, and at all times mentioned herein was, an individual
 13 citizen of the State of Nevada.

14 16. Plaintiff is a patient of ADG and has been a patient of ADG since 2008. Plaintiff
 15 routinely has provided Private Information to ADG in connection with receiving ADG's services.
 16 In requesting, requiring and maintaining Plaintiff's Private Information for its business purposes,
 17 ADG impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's
 18 Private Information. ADG did not take proper care of Plaintiff's Private Information, leading to its
 19 theft as a direct result of ADG's inadequate security measures and data protection protocols.

20 17. Once Private Information is exposed, there is virtually no way to ensure that the
 21 exposed information has been fully recovered or contained against future misuse. For this reason,
 22 Plaintiff will need to maintain heightened measures for years, and possibly for life.

23 18. On information and belief, following the Data Breach, Plaintiff was a victim of
 24 identity theft, in which an unauthorized individual opened a PayPal account in Plaintiff's name,
 25 and incurred charges or debt associated with that account.

26 19. Plaintiff also suffered actual injury from having Private Information compromised
 27 as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the
 28 value of Plaintiff's confidential Private Information—a form of property that Plaintiff entrusted to

1 ADG, which was compromised as a result of the Data Breach and (b) a violation of Plaintiff's
2 privacy rights as a result of unauthorized disclosure of Private Information.

3 20. Had Plaintiff known that ADG does not adequately protect Private Information,
4 Plaintiff would not have used ADG's services nor agreed to provide ADG with Private
5 Information.

6 21. As a result of ADG's failure to adequately safeguard Plaintiff's Private
7 Information, Plaintiff has been injured. Plaintiff also is at a continued risk of harm because
8 Plaintiff's Private Information remains in ADG's systems, which have already been shown to be
9 susceptible to compromise and attack, and is subject to further attack so long as Defendant fails to
10 undertake the necessary and appropriate data security measures to protect the Private Information
11 in its possession.

12 | Defendant

Absolute Dental Group, LLC

14 22. Defendant ADG is a dental services practice and provider and a Delaware
15 corporation with its principal place of business located at 8370 W. Cheyenne Ave Ste. 103, Las
16 Vegas, NV 89129.

III. JURISDICTION AND VENUE

18 23. This Court has subject matter jurisdiction over this action under the Class Action
19 Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the
20 aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000
21 exclusive of interest and costs, and, upon information and belief, members of the proposed Class
22 are citizens of states different from Defendant.

23 24. This Court has jurisdiction over Defendant through its business operations in this
24 District, the specific nature of which occurs in this District. Defendant intentionally avails itself of
25 the markets within this District to render the exercise of jurisdiction by this Court just and proper.

26 25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a
27 substantial part of the events and omissions giving rise to this action occurred in this District, and
28 because Defendant resides in this judicial district.

IV. FACTUAL ALLEGATIONS

A. ADG's Business and Collection of Plaintiff's and Class Members' Private Information

26. ADG is a Nevada based dental service organization with over fifty locations.² ADG provides comprehensive dental services ranging from general dental and hygienist services to orthodontics, oral surgery, pedodontics, and endodontics.³ ADG generates approximately \$44 million in annual revenue.

27. As a condition of receiving services, ADG requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from ADG, Plaintiff and Class Members were required to provide their Private Information to Defendant.

28. In its Privacy Policy, ADG states that “[y]our information, whether public or private, will not be sold, exchanged, transferred, or given to any other company for any reason whatsoever, without your consent, other than for the express purpose of delivering the purchased product or service requested.”⁴

29. Due to the highly sensitive and personal nature of the information ADG acquires and stores with respect to its patients, ADG, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

² Connect With a Trusted General Dentist in Nevada, Absolute Dental, <https://www.absolutedental.com/about/general-dentists/> (last visited June 2, 2025).

³ About, Absolute Dental, <https://www.absolutedental.com/about/> (last visited June 2, 2025).

⁴ Privacy Policy, Absolute Dental, <https://www.absolutedental.com/privacy-policy/> (last visited June 2, 2025).

1 30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class
 2 Members' Private Information, ADG assumed legal and equitable duties it owed to them and knew
 3 or should have known that it was responsible for protecting Plaintiff's and Class Members' Private
 4 Information from unauthorized disclosure and exfiltration.

5 31. Plaintiff and Class Members relied on ADG to keep their Private Information
 6 confidential and securely maintained and to only make authorized disclosures of this Information,
 7 which Defendant ultimately failed to do.

8 **B. The Data Breach**

9 32. Little information is available concerning the Data Breach, and ADG has provided
 10 scant details about it outside of the filing it made with HHS OCR on May 2, 2025.

11 33. According to the HHS OCR notice, the Data Breach involved a hacking/IT Incident
 12 on ADG's network server.⁵

13 34. Per ADG's report on the HHS OCR website, ADG identifies that 501 individuals
 14 have been impacted by the Data Breach. On information and belief, this number is substantially
 15 higher, and the 501 individuals figure is simply a placeholder figure. Indeed, the HHS OCR data
 16 breach reporting portal makes clear that “[a]s required by section 13402(e)(4) of the HITECH Act,
 17 the Secretary must post a list of breaches of unsecured protected health information affecting 500
 18 or more individuals.”⁶

19 35. On information and belief, the information disclosed during the Data Breach
 20 includes some or all of the following information, and potentially other sensitive information:
 21 names, dates of birth, health information, dental information and records, doctor's name, health
 22 and/or dental insurance information, medical billing or claims information, prescription or
 23 medication information, Social Security numbers, and treatment information.

24 36. To date, Defendant has failed to disclose crucial details like the root cause of the
 25 Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a
 26

27 ⁵ *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health
 28 Information, supra.*

⁶ *Id.*

1 breach does not occur again. To date, these critical facts have not been explained or clarified to
 2 Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information
 3 is protected.

4 37. Thus, ADG's purported disclosure to HHS OCR amounts to no real disclosure at
 5 all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any
 6 degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the
 7 harms resulting from the Data Breach was and is severely diminished.

8 38. In addition, ADG offers no substantive steps to help victims like Plaintiff and Class
 9 Members to protect themselves.

10 39. ADG had obligations created by contract, industry standards, common law, and
 11 representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members'
 12 Private Information confidential and to protect it from unauthorized access and disclosure.

13 40. Plaintiff and Class Members provided their Private Information to ADG with the
 14 reasonable expectation and mutual understanding that ADG would comply with its obligations to
 15 keep such information confidential and secure from unauthorized access and to provide timely
 16 notice of any security breaches.

17 41. ADG's data security obligations were particularly important given the substantial
 18 increase in cyberattacks in recent years.

19 42. ADG knew or should have known that its electronic records would be targeted by
 20 cybercriminals.

21 **C. Defendant Knew or Should Have Known of the Risk Because Institutions in
 22 Possession of Private Information are Particularly Susceptible to
 23 Cyberattacks**

24 43. Defendant's data security obligations were particularly important given the
 25 substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and
 26 store Private Information, like Defendant.

27 44. Data thieves regularly target institutions like Defendant due to the highly sensitive
 28 information in their custody. Defendant knew and understood that unprotected Private Information

1 is valuable and highly sought after by criminal parties who seek to illegally monetize that Private
2 Information through unauthorized access.

3 45. In 2021, a record 3,205 data breaches occurred, resulting in approximately
4 353,027,892 individuals being compromised, a 78% increase from 2022.⁷

5 46. In light of recent high profile data breaches at other healthcare providers, Defendant
6 knew or should have known that the Private Information it collected and maintained would be
7 targeted by cybercriminals.

8 47. As a custodian of Private Information, Defendant knew, or should have known, the
9 importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members,
10 and of the foreseeable consequences if its data security systems were breached, including the
11 significant costs imposed on Plaintiff and Class Members as a result of a breach.

12 48. Despite the prevalence of public announcements of data breach and data security
13 compromises, Defendant failed to take appropriate steps to protect the Private Information of
14 Plaintiff and Class Members from being compromised.

15 49. Defendant was, or should have been, fully aware of the unique type and the
16 significant volume of data on Defendant's server(s), amounting to potentially tens or hundreds of
17 thousands of individuals' detailed, Private Information, and, thus, the significant number of
18 individuals who would be harmed by the exposure of the unencrypted data.

19 50. The injuries to Plaintiff and Class Members were directly and proximately caused
20 by Defendant's failure to implement or maintain adequate data security measures for the Private
21 Information of Plaintiff and Class Members.

22 51. The ramifications of Defendant's failure to keep secure the Private Information of
23 Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen,
24 fraudulent use of that information and damage to victims may continue for years.

25
26
27 7 *ITRC 2023 Data Breach Report – Key Findings and Solutions*, Bluefin,
28 <https://www.bluefin.com/bluefin-news/itrc-2023-data-breach-report-key-findings-and-solutions/>
(last visited Apr. 17, 2025).

1 **D. Value of Personally Identifiable Information**

2 52. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
 3 committed or attempted using the identifying information of another person without authority.”⁸
 4 The FTC describes “identifying information” as “any name or number that may be used, alone or
 5 in conjunction with any other information, to identify a specific person,” including, among other
 6 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s
 7 license or identification number, alien registration number, government passport number,
 8 employer or taxpayer identification number.”⁹

9 53. The Private Information of individuals remains of high value to criminals, as
 10 evidenced by the prices they will pay through the dark web. Numerous sources cite dark web
 11 pricing for stolen identity credentials.¹⁰

12 54. For example, Private Information can be sold at a price ranging from \$40 to \$200.¹¹
 13 Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹²

14 55. Theft of PHI is also gravely serious: “[a] thief may use your name or health
 15 insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,
 16 or get other care. If the thief’s health information is mixed with yours, your treatment, insurance
 17 and payment records, and credit report may be affected.”¹³

18 56. The greater efficiency of electronic health records brings the risk of privacy
 19 breaches. These electronic health records contain a lot of sensitive information (e.g., patient data,
 20 patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to

21
 22 ⁸ 17 C.F.R. § 248.201 (2013).
 23 ⁹ *Id.*

24 ¹⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, DIGITAL TRENDS
 25 (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

26 ¹¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec.
 27 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

28 ¹² *In the Dark*, VPNOVERVIEW, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited June 2, 2025).

29 ¹³ *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187>
 (last visited June 2, 2025).

1 cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web.
 2 As such, Private Information is a valuable commodity for which a "cyber black market" exists
 3 where criminals openly post stolen payment card numbers, Social Security numbers, and other
 4 personal information on several underground internet websites. Unsurprisingly, the health care
 5 industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

6 57. Between 2005 and 2019, at least 249 million people were affected by health care
 7 data breaches.¹⁴ Indeed, during 2019 alone, over 41 million health care records were exposed,
 8 stolen, or unlawfully disclosed in 505 data breaches.¹⁵ In short, these sorts of data breaches are
 9 increasingly common, especially among health care systems, which account for 30.03 percent of
 10 overall health data breaches, according to cybersecurity firm Tenable.¹⁶

11 58. According to account monitoring company LogDog, medical data sells for \$50 and
 12 up on the dark web.¹⁷

13 59. "Medical identity theft is a growing and dangerous crime that leaves its victims
 14 with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy
 15 Forum. "Victims often experience financial repercussions and worse yet, they frequently discover
 16 erroneous information has been added to their personal medical files due to the thief's activities."¹⁸

17 60. A study by Experian found that the average cost of medical identity theft is "about
 18 \$20,000" per incident and that most victims of medical identity theft were forced to pay out-of-
 19

21 ¹⁴ Adil Hussain She Et Al., *Healthcare Data Breaches: Insights and Implications* (2020),
 22 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

23 ¹⁵ Steve Alder, *December 2019 Healthcare Data Breach Report*, The HIPAA Journal (Jan. 21,
 24 2020), <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/>.

25 ¹⁶ Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era
 Breaches*, Tenable (Mar. 10, 2021), <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches>.

26 ¹⁷ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security
 27 (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

28 ¹⁸ Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7,
 29 2014), <https://khn.org/news/rise-of-identity-theft/>.

1 pocket costs for health care they did not receive to restore coverage.¹⁹ Almost half of medical
 2 identity theft victims lose their health care coverage as a result of the incident, while nearly one-
 3 third of medical identity theft victims saw their insurance premiums rise, and 40 percent were
 4 never able to resolve their identity theft at all.²⁰

5 61. Based on the foregoing, the information compromised in the Data Breach is
 6 significantly more valuable than the loss of, for example, credit card information in a retailer data
 7 breach because, there, victims can cancel or close credit and debit card accounts. The information
 8 compromised in this Data Breach—PHI and names—is impossible to “close” and difficult, if not
 9 impossible, to change.

10 62. This data demands a much higher price on the black market. Martin Walter, senior
 11 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
 12 personally identifiable information . . . [is] worth more than 10x on the black market.”²¹

13 63. Among other forms of fraud, identity thieves may obtain driver’s licenses,
 14 government benefits, medical services, and housing or even give false information to police.

15 64. The fraudulent activity resulting from the Data Breach may not come to light for
 16 years. There may be a time lag between when harm occurs versus when it is discovered, and also
 17 between when Private Information is stolen and when it is used. According to the U.S. Government
 18 Accountability Office (“GAO”), which conducted a study regarding data breaches:

19 [Law enforcement officials told us that in some cases, stolen data
 20 may be held for up to a year or more before being used to commit
 21 identity theft. Further, once stolen data have been sold or posted on
 the Web, fraudulent use of that information may continue for years.]

24 ¹⁹ See Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010),
 25 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

26 ²⁰ *Id.*

27 ²¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card
 28 Numbers*, IT WORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

1 As a result, studies that attempt to measure the harm resulting from
 2 data breaches cannot necessarily rule out all future harm.^[22]

3 **E. Defendant Failed to Comply with FTC Guidelines**

4 65. The FTC has promulgated numerous guides for businesses which highlight the
 5 importance of implementing reasonable data security practices. According to the FTC, the need
 6 for data security should be factored into all business decision making. Indeed, the FTC has
 7 concluded that a company's failure to maintain reasonable and appropriate data security for
 8 consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the
 9 FTCA, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

10 66. In October 2016, the FTC updated its publication, *Protecting Personal*
 11 *Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The
 12 guidelines note that businesses should protect the personal consumer information they keep,
 13 properly dispose of personal information that is no longer needed, encrypt information stored on
 14 computer networks, understand their network's vulnerabilities, and implement policies to correct
 15 any security problems. The guidelines also recommend that businesses use an intrusion detection
 16 system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating
 17 someone is attempting to hack into the system, watch for large amounts of data being transmitted
 18 from the system, and have a response plan ready in the event of a breach.

19 67. The FTC further recommends that companies not maintain Private Information
 20 longer than is needed for authorization of a transaction, limit access to sensitive data, require
 21 complex passwords to be used on networks, use industry-tested methods for security, monitor the
 22 network for suspicious activity, and verify that third-party service providers have implemented
 23 reasonable security measures.

24 68. The FTC has brought enforcement actions against businesses for failing to
 25 adequately and reasonably protect consumer data by treating the failure to employ reasonable and
 26 appropriate measures to protect against unauthorized access to confidential consumer data as an

27 22 *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf>.

1 unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify
 2 the measures businesses must take to meet their data security obligations.

3 69. As evidenced by the Data Breach, Defendant failed to properly implement basic
 4 data security practices and failed to audit, monitor, or ensure the integrity of its data security
 5 practices. Defendant's failure to employ reasonable and appropriate measures to protect against
 6 unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair
 7 act or practice prohibited by Section 5 of the FTCA.

8 70. Defendant was at all times fully aware of its obligation to protect the Private
 9 Information of consumers under the FTCA, yet failed to comply with such obligations. Defendant
 10 was also aware of the significant repercussions that would result from its failure to do so.
 11 Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of
 12 Private Information it obtained and stored and the foreseeable consequences of the immense
 13 damages that would result to Plaintiff and the Class.

14 **F. Defendant Failed to Comply with HIPAA**

15 71. On information and belief, Defendant is a covered entity under HIPAA (45 C.F.R.
 16 § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.
 17 Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health
 18 Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected
 19 Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

20 72. On information and belief, Defendant is subject to the rules and regulations for
 21 safeguarding electronic forms of medical information pursuant to the Health Information
 22 Technology Act ("HITECH"). See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

23 73. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health
 24 Information establishes national standards for the protection of health information.

25 74. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic
 26 Protected Health Information establishes a national set of security standards for protecting health
 27 information that is kept or transferred in electronic form.

1 75. HIPAA requires “comply[ance] with the applicable standards, implementation
2 specifications, and requirements” of HIPAA “with respect to electronic protected health
3 information.” 45 C.F.R. § 164.302.

4 76. “Electronic protected health information” is “individually identifiable health
5 information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45
6 C.F.R. § 160.103.

7 77. HIPAA’s Security Rule requires Defendant to do the following:

- 8 a. Ensure the confidentiality, integrity, and availability of all electronic protected
9 health information the covered entity or business associate creates, receives,
10 maintains, or transmits;
- 11 b. Protect against any reasonably anticipated threats or hazards to the security or
12 integrity of such information;
- 13 c. Protect against any reasonably anticipated uses or disclosures of such information
14 that are not permitted; and
- 15 d. Ensure compliance by its workforce.

16 78. HIPAA also requires Defendant to “review and modify the security measures
17 implemented . . . as needed to continue provision of reasonable and appropriate protection of
18 electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is
19 required under HIPAA to “[i]mplement technical policies and procedures for electronic
20 information systems that maintain electronic protected health information to allow access only to
21 those persons or software programs that have been granted access rights.” 45 C.F.R. §
22 164.312(a)(1).

23 79. HIPAA and HITECH also obligated Defendant to implement policies and
24 procedures to prevent, detect, contain, and correct security violations, and to protect against uses
25 or disclosures of electronic protected health information that are reasonably anticipated but not
26 permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42
27 U.S.C. §17902.

1 80. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires
2 Defendant to provide notice of the Data Breach to each affected individual “without unreasonable
3 delay and in no case later than 60 days following discovery of the breach.”

4 81. HIPAA requires a covered entity to have and apply appropriate sanctions against
5 members of its workforce who fail to comply with the privacy policies and procedures of the
6 covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. §
7 164.530(e).

8 82. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful
9 effect that is known to the covered entity of a use or disclosure of protected health information in
10 violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by
11 the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

12 83. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of
13 Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in
14 the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed
15 guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost
16 effective and appropriate administrative, physical, and technical safeguards to protect the
17 confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements
18 of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance
19 Material. The list of resources includes a link to guidelines set by the National Institute of
20 Standards and Technology (NIST), which OCR says “represent the industry standard for good
21 business practices with respect to standards for securing e-PHI.” US Department of Health &
22 Human Services, Guidance on Risk Analysis.

23 84. Defendant was at all times fully aware of its HIPAA obligations to protect the
24 Private Information of consumers yet failed to comply with such obligations. Defendant was also
25 aware of the significant repercussions that would result from its failure to do so. Accordingly,
26 Defendant’s conduct was particularly unreasonable given the nature and amount of Private
27 Information it obtained and stored and the foreseeable consequences of the immense damages that
28 would result to Plaintiff and the Class.

1 **G. Defendant Failed to Comply with Industry Standards**

2 85. Experts studying cybersecurity routinely identify health care providers like
 3 Defendant as being particularly vulnerable to cyberattacks because of the value of the Private
 4 Information which they collect and maintain.

5 86. Some industry best practices that should be implemented by institutions dealing
 6 with sensitive Private Information, like Defendant, include, but are not limited to: educating all
 7 employees, strong password requirements, multilayer security including firewalls, anti-virus and
 8 anti-malware software, encryption, multi-factor authentication, backing up data, and limiting
 9 which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to
 10 follow some or all of these industry best practices.

11 87. Other best cybersecurity practices that are standard within healthcare networks that
 12 store Private Information include: installing appropriate malware detection software; monitoring
 13 and limiting network ports; protecting web browsers and email management systems; setting up
 14 network systems such as firewalls, switches, and routers; monitoring and protecting physical
 15 security systems; and training staff regarding these points. As evidenced by the Data Breach,
 16 Defendant failed to follow these cybersecurity best practices.

17 88. Defendant failed to implement industry-standard cybersecurity measures, including
 18 by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0
 19 (including PR-AA-01, PR-AA.-02, PR-AA-03, PR-AA-04, PR-AA-05, PR.AT-01, PR.DS-01, PR-
 20 DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-
 21 06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls
 22 (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by
 23 failing to comply with other industry standards for protecting Plaintiff's and Class Members'
 24 Private Information, resulting in the Data Breach.

25 89. Defendant failed to comply with these accepted standards, thereby permitting the
 26 Data Breach to occur.

1 **H. Defendant Breached Its Duty to Safeguard Plaintiff's and Class Members'**
2 **Private Information**

3 90. In addition to its obligations under federal laws, Defendant owed duties to Plaintiff
4 and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding,
5 deleting, and protecting the Private Information in its possession from being compromised, lost,
6 stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and
7 Class Members to provide reasonable security, including consistency with industry standards and
8 requirements, and to ensure that its computer systems, networks, and protocols adequately
9 protected the Private Information of Class Members.

10 91. Defendant breached its obligations to Plaintiff and Class Members and/or was
11 otherwise negligent and reckless because it failed to properly maintain and safeguard its computer
12 systems and data and failed to audit, monitor, or ensure the integrity of its data security practices.
13 Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- 14 a. Failing to maintain an adequate data security system that would reduce the risk of data
15 breaches and cyberattacks;
- 16 b. Failing to adequately protect consumers' Private Information;
- 17 c. Failing to properly monitor its own data security systems for existing intrusions;
- 18 d. Failing to adhere to industry standards for cybersecurity as discussed above; and
- 19 e. Otherwise breaching its duties and obligations to protect Plaintiff's and Class
20 Members' Private Information.

21 92. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class
22 Members' Private Information by allowing cyberthieves to access its computer network and
23 systems, which contained unsecured and unencrypted Private Information.

24 93. Had Defendant remedied the deficiencies in its information storage and security
25 systems, followed industry guidelines, and adopted security measures recommended by experts in
26 the field, it could have prevented intrusion into its information storage and security systems and,
27 ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

1 **I. Plaintiff and Class Members Suffered Common Injuries and Damages**

2 94. As a result of Defendant's ineffective and inadequate data security practices, the
 3 Data Breach, and the foreseeable consequences of Private Information ending up in the possession
 4 of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is
 5 imminent, and Plaintiff and Class Members have all sustained actual injuries and damages,
 6 including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the
 7 materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain
 8 (price premium damages); (d) diminution of value of their Private Information; (e) invasion of
 9 privacy; and (f) the continued risk to their Private Information, which remains in the possession of
 10 Defendant, and which is subject to further breaches, so long as Defendant fails to undertake
 11 appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

12 ***Increased and Imminent Risk of Identity Theft***

13 95. Plaintiff and Class Members are at a heightened risk of identity theft for years to
 14 come as a result of the Data Breach.

15 96. The unencrypted Private Information of Class Members will end up for sale on the
 16 dark web because that is the *modus operandi* of cybercriminals that commit attacks of this type.
 17 In addition, unencrypted Private Information may fall into the hands of companies that will use
 18 the detailed Private Information for targeted marketing without the approval of Plaintiff and Class
 19 Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class
 20 Members.

21 97. The link between a data breach and the risk of identity theft is simple and well
 22 established. Criminals acquire and steal Private Information to monetize the information.
 23 Criminals monetize the data by selling the stolen information on the black market to other
 24 criminals who then utilize the information to commit a variety of identity theft related crimes
 25 discussed below.

26 98. Because a person's identity is akin to a puzzle with multiple data points, the more
 27 accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take
 28

1 on the victim's identity—or track the victim to attempt other hacking crimes against the individual
 2 to obtain more data to perfect a crime.

3 99. For example, armed with just a name and date of birth, a data thief can utilize a
 4 hacking technique referred to as “social engineering” to obtain even more information about a
 5 victim’s identity, such as a person’s login credentials or Social Security number. Social
 6 engineering is a form of hacking whereby a data thief uses previously acquired information to
 7 manipulate and trick individuals into disclosing additional confidential or personal information
 8 through means such as spam phone calls and text messages or phishing emails. Data breaches can
 9 be the starting point for these additional targeted attacks on the victim.

10 100. One such example of criminals piecing together bits and pieces of compromised
 11 Private Information for profit is the development of “Fullz” packages.²³

12 101. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private
 13 Information to marry unregulated data available elsewhere to criminally stolen data with an
 14 astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on
 15 individuals.

16 102. The development of “Fullz” packages means here that the stolen Private
 17 Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class
 18 Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other
 19 words, even if certain information such as emails, phone numbers, or credit card numbers may not

20

21 ²³ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not
 22 limited to, the name, address, credit card information, social security number, date of birth, and
 23 more. As a rule of thumb, the more information you have on a victim, the more money that can be
 24 made off those credentials. Fullz are usually pricier than standard credit card credentials,
 25 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning
 26 credentials into money) in various ways, including performing bank transactions over the phone
 27 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials
 28 associated with credit cards that are no longer valid, can still be used for numerous purposes,
 including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule
 account” (an account that will accept a fraudulent money transfer from a compromised account)
 without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground
 Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014),
<https://krebsongsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm>.

1 be included in the Private Information that was exfiltrated in the Data Breach, criminals may still
2 easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals
3 (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

5 103. As a result of the recognized risk of identity theft, when a data breach occurs, and
6 an individual is notified by a company that their Private Information was compromised, as in this
7 Data Breach, the reasonable person is expected to take steps and spend time to address the
8 dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim
9 of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports
10 could expose the individual to greater financial harm—yet, the resource and asset of time has been
11 lost.

12 104. Plaintiff and Class Members have spent, and will spend additional time in the
13 future, on a variety of prudent actions to remedy the harms they have or may experience as a result
14 of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing
15 passwords and re-securing their own computer networks; and checking their financial accounts
16 and health insurance statements for any indication of fraudulent activity, which may take years to
17 detect.

18 105. These efforts are consistent with the U.S. Government Accountability Office's
19 2007 report regarding data breaches ("GAO Report"), in which it noted that victims of identity
20 theft will face "substantial costs and time to repair the damage to their good name and credit
21 record."²⁴

106. These efforts are also consistent with the steps that FTC recommends that data
breach victims take to protect their personal and financial information after a data breach,
including: contacting one of the credit bureaus to place a fraud alert (and considering an extended
fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

²⁷ ²⁸ *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office, GAO-07-737, (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

1 contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on
 2 their credit, and correcting their credit reports.²⁵

3 ***Diminished Value of Private Information***

4 107. PII and PHI are valuable property rights.²⁶ Their value is axiomatic, considering
 5 the value of Big Data in corporate America and the consequences of cyber thefts include heavy
 6 prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private
 7 Information has considerable market value.

8 108. An active and robust legitimate marketplace for Private Information exists. In 2019,
 9 the data brokering industry was worth roughly \$200 billion.²⁷

10 109. In fact, the data marketplace is so sophisticated that consumers can actually sell
 11 their non-public information directly to a data broker who in turn aggregates the information and
 12 provides it to marketers or app developers.²⁸

13 110. Consumers who agree to provide their web browsing history to the Nielsen
 14 Corporation can receive up to \$50.00 a year.²⁹

15 111. As a result of the Data Breach, Plaintiff's and Class Members' Private Information,
 16 which has an inherent market value in both legitimate and dark markets, has been damaged and
 17 diminished by its compromise and unauthorized release. However, this transfer of value occurred
 18 without any consideration paid to Plaintiff or Class Members for their property, resulting in an
 19 economic loss. Moreover, the Private Information is now readily available, and the rarity of the
 20 Data has been lost, thereby causing additional loss of value.

21 ²⁵ See *Identity Theft.gov*, FEDERAL TRADE COMMISSION, <https://www.identitytheft.gov/Steps> (last
 22 visited June 3, 2025).

23 ²⁶ See, e.g., John T. Soma Et Al., *Corporate Privacy Trend: The “Value” of Personally*
 24 *Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH.
 25 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is
 rapidly reaching a level comparable to the value of traditional financial assets.”) (citations
 omitted).

26 ²⁷ David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, Los Angeles
 Times (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

27 ²⁸ Main Page, <https://datacoup.com/> (last visited June 3, 2025).

28 ²⁹ *Frequently Asked Questions*, Nielsen Computer & Mobile Panel,
<https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited June 3, 2025).

1 112. At all relevant times, Defendant knew, or reasonably should have known, of the
2 importance of safeguarding the Private Information of Plaintiff and Class Members, and of the
3 foreseeable consequences that would occur if their data security systems were breached, including,
4 specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result
5 of a breach.

6 113. Defendant was, or should have been, fully aware of the unique type and the
7 significant volume of data on its network, which upon information and belief, amounts to tens or
8 hundreds of thousands of individuals' Private Information, and thus, the significant number of
9 individuals who would be harmed by the exposure of the unencrypted data.

10 114. The injuries to Plaintiff and Class Members were directly and proximately caused
11 by Defendant's failure to implement or maintain adequate data security measures for the Private
12 Information of Plaintiff and Class Members.

13 **J. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and
14 Necessary.**

15 115. Given the type of targeted attack in this case and sophisticated criminal activity, the
16 type of Private Information involved, and the volume of data obtained in the Data Breach, there is
17 a strong probability that entire batches of stolen information have been placed, or will be placed,
18 on the black market/dark web for sale and purchase by criminals intending to utilize the Private
19 Information for identity theft crimes.

20 116. Such fraud may go undetected for years; consequently, Plaintiff and Class Members
21 are at a present and continuous risk of fraud and identity theft for many years into the future.

22 117. The retail cost of credit monitoring and identity theft monitoring can cost around
23 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class
24 Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a
25 minimum of five years that Plaintiff and Class Members would not need to bear but for
26 Defendant's failure to safeguard their Private Information.

27
28

V. CLASS ACTION ALLEGATIONS

118. Plaintiff brings this action individually, and on behalf of all members of the following Classes (together, the “Class” or “Classes”) of similarly situated persons:

Nationwide Class

All persons residing in the United States whose Private Information was compromised in the Data Breach disclosed by Absolute Dental Group, LLC, including all who were sent notice of the Data Breach.

Nevada Class

All persons residing in the state of Nevada whose Private Information was compromised in the Data Breach disclosed by Absolute Dental Group, LLC, including all who were sent notice of the Data Breach.

119. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

120. Plaintiff reserves the right to modify or amend the definitions of the proposed
Classes, before the Court determines whether certification is appropriate.

121. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

122. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of tens or hundreds of thousands of patients of ADG who are geographically dispersed, including in states beyond Nevada, whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through ADG's records, Class Members' records, publication notice, self-identification, and other means.

123. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether ADG engaged in the conduct alleged herein;

- b. Whether ADG's conduct violated the FTCA and HIPAA;
- c. When ADG learned of the Data Breach
- d. Whether ADG's response to the Data Breach was adequate;
- e. Whether ADG unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;
- f. Whether ADG failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether ADG's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether ADG's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether ADG owed a duty to Class Members to safeguard their Private Information;
- j. Whether ADG breached its duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether ADG had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether ADG breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- n. Whether ADG knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of ADG's misconduct;
- p. Whether ADG's conduct was negligent;
- q. Whether ADG's conduct was per se negligent;

- 1 r. Whether ADG's conduct constitutes a breach of contract;
- 2 s. Whether ADG's conduct constitutes a breach of implied contract;
- 3 t. Whether ADG was unjustly enriched;
- 4 u. Whether ADG's conduct constitutes a breach of fiduciary duty;
- 5 v. Whether ADG's conduct constitutes a breach of confidence;
- 6 w. Whether Plaintiff and Class Members are entitled to actual and/or statutory
7 damages;
- 8 x. Whether Plaintiff and Class Members are entitled to credit or identity
9 monitoring and monetary relief; and
- 10 y. Whether Plaintiff and Class Members are entitled to equitable relief,
11 including injunctive relief, restitution, disgorgement, and/or the
12 establishment of a constructive trust.

13 124. ADG engaged in a common course of conduct giving rise to the legal rights sought
14 to be enforced by Plaintiff individually and on behalf of all other class members. Individual
15 questions, if any, pale in comparison, in both quantity and quality, to the numerous common
16 questions that dominate this action.

17 125. Typicality. Plaintiff's claims are typical of those of other Class Members because
18 Plaintiff's Private Information, like that of every other Class Member, was compromised in the
19 Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*,
20 all Class Members were injured through the common misconduct of ADG. Plaintiff is advancing
21 the same claims and legal theories on behalf of Plaintiff and all other Class Members, and there
22 are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members
23 arise from the same operative facts and are based on the same legal theories.

24 126. Adequacy of Representation. Plaintiff will fairly and adequately represent and
25 protect the interests of Class Members. Plaintiff's counsel is competent and experienced in
26 litigating class actions, including data privacy litigation of this kind.

27 127. Predominance. ADG has engaged in a common course of conduct toward Plaintiff
28 and Class Members in that all of Plaintiff's and Class Members' data was stored on the same

1 computer systems and unlawfully accessed and exfiltrated in the same way. The common issues
2 arising from ADG's conduct affecting Class Members set out above predominate over any
3 individualized issues. Adjudication of these common issues in a single action has important and
4 desirable advantages of judicial economy.

5 128. Superiority. A class action is superior to other available methods for the fair and
6 efficient adjudication of this controversy and no unusual difficulties are likely to be encountered
7 in the management of this class action. Class treatment of common questions of law and fact is
8 superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class
9 Members would likely find that the cost of litigating their individual claims is prohibitively high
10 and would therefore have no effective remedy. The prosecution of separate actions by individual
11 Class Members would create a risk of inconsistent or varying adjudications with respect to
12 individual Class Members, which would establish incompatible standards of conduct for ADG. In
13 contrast, conducting this action as a class action presents far fewer management difficulties,
14 conserves judicial resources and the parties' resources, and protects the rights of each Class
15 Member.

16 129. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). ADG has acted
17 and/or refused to act on grounds generally applicable to the Class such that final injunctive relief
18 and/or corresponding declaratory relief is appropriate as to the Class as a whole.

19 130. Finally, all members of the proposed Class are readily ascertainable. ADG has
20 access to the names and addresses and/or email addresses of Class Members affected by the Data
21 Breach. Class Members have already been preliminarily identified and sent notice of the Data
22 Breach by ADG.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

131. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
set forth herein.

1 132. ADG knowingly collected, came into possession of, and maintained Plaintiff's and
2 Class Members' Private Information. ADG had a duty to exercise reasonable care in safeguarding,
3 securing, and protecting the Private Information from being disclosed, compromised, lost, stolen,
4 and misused by unauthorized parties.

5 133. ADG's duty also included the responsibility to implement processes by which it
6 could quickly detect and analyze a breach of its security systems, and give prompt notice to those
7 affected in the event of a cyberattack.

8 134. ADG knew or should have known of the risks inherent in collecting the Private
9 Information of Plaintiff and Class Members and the importance of adequate security. ADG was
10 on notice because, on information and belief, it knew or should have known that it would be an
11 attractive target for cyberattacks.

12 135. ADG owed a duty of care to Plaintiff and Class Members whose Private
13 Information was entrusted to it. ADG's duties included, but were not limited to, the following:

- 14 a. To exercise reasonable care in obtaining, retaining, securing, safeguarding,
15 deleting, and protecting Private Information in its possession;
- 16 b. To protect patients' Private Information using reasonable and adequate security
17 procedures and systems compliant with industry standards;
- 18 c. To have procedures in place to prevent the loss or unauthorized dissemination
19 of Private Information in its possession;
- 20 d. To employ reasonable security measures and otherwise protect the Private
21 Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;
- 22 e. To implement processes to quickly detect a data breach and to timely act on
23 warnings about data breaches; and
- 24 f. To promptly notify Plaintiff and Class Members of the Data Breach, and to
25 precisely disclose the type(s) of information compromised.

26 136. ADG's duty to employ reasonable data security measures arose, in part, under
27 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .
28

1 practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair
 2 practice of failing to use reasonable measures to protect confidential data.

3 137. ADG’s duty also arose because Defendant was bound by industry standards to
 4 protect its patients’ confidential Private Information.

5 138. Plaintiff and Class Members were foreseeable victims of any inadequate security
 6 practices on the part of Defendant, and ADG owed them a duty of care to not subject them to an
 7 unreasonable risk of harm.

8 139. ADG, through its actions and/or omissions, unlawfully breached its duty to Plaintiff
 9 and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff’s
 10 and Class Members’ Private Information within ADG’s possession.

11 140. ADG, by its actions and/or omissions, breached its duty of care by failing to
 12 provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and
 13 data security practices to safeguard the Private Information of Plaintiff and Class Members.

14 141. ADG, by its actions and/or omissions, breached its duty of care by failing to
 15 promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to
 16 the persons whose Private Information was compromised.

17 142. ADG breached its duties, and thus was negligent, by failing to use reasonable
 18 measures to protect Class Members’ Private Information. The specific negligent acts and
 19 omissions committed by Defendant include, but are not limited to, the following:

- 20 a. Failing to adopt, implement, and maintain adequate security measures to safeguard
 Class Members’ Private Information;
- 22 b. Failing to adequately monitor the security of its networks and systems;
- 23 c. Failing to periodically ensure that its email system maintained reasonable data
 security safeguards;
- 25 d. Allowing unauthorized access to Class Members’ Private Information;
- 26 e. Failing to comply with the FTCA; and
- 27 f. Failing to timely notify Class Members about the Data Breach so that they could
 take appropriate steps to mitigate the potential for identity theft and other damages.

1 143. ADG acted with reckless disregard for the rights of Plaintiff and Class Members by
2 failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and
3 Class Members could take measures to protect themselves from damages caused by the fraudulent
4 use of the Private Information compromised in the Data Breach.

5 144. ADG had a special relationship with Plaintiff and Class Members. Plaintiff's and
6 Class Members' willingness to entrust ADG with their Private Information was predicated on the
7 understanding that ADG would take adequate security precautions. Moreover, only ADG had the
8 ability to protect its systems (and the Private Information that it stored on them) from attack.

9 145. ADG's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and
10 Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged
11 herein.

12 146. As a result of ADG's ongoing failure to notify Plaintiff and Class Members
13 regarding exactly what Private Information has been compromised, Plaintiff and Class Members
14 have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

15 147. ADG's breaches of duty also caused a substantial, imminent risk to Plaintiff and
16 Class Members of identity theft, loss of control over their Private Information, and/or loss of time
17 and money to monitor their accounts for fraud.

18 148. As a result of ADG's negligence in breach of its duties owed to Plaintiff and Class
19 Members, Plaintiff and Class Members are in danger of imminent harm in that their Private
20 Information, which is still in the possession of third parties, will be used for fraudulent purposes.

21 149. ADG also had independent duties under state laws that required it to reasonably
22 safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the
23 Data Breach.

24 150. As a direct and proximate result of ADG's negligent conduct, Plaintiff and Class
25 Members have suffered damages as alleged herein and are at imminent risk of further harm.

26 151. The injury and harm that Plaintiff and Class Members suffered was reasonably
27 foreseeable.

1 152. Plaintiff and Class Members have suffered injury and are entitled to damages in an
2 amount to be proven at trial.

3 153. In addition to monetary relief, Plaintiff and Class Members are also entitled to
4 injunctive relief requiring ADG to, *inter alia*, strengthen its data security systems and monitoring
5 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
6 identity theft insurance to Plaintiff and Class Members.

COUNT II

NEGLIGENCE PER SE

9 154. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
10 set forth herein.

11 155. Pursuant to Section 5 of the FTCA, ADG had a duty to provide fair and adequate
12 computer systems and data security to safeguard the Private Information of Plaintiff and Class
13 Members.

14 156. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq.*, ADG had a duty to implement
15 reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

16 157. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI
17 it maintained unusable, unreadable, or indecipherable to unauthorized individuals by “the use of
18 an algorithmic process to transform data into a form in which there is a low probability of assigning
19 meaning without the use of a confidential process or key.” *See* definition of “encryption” at 45
20 C.F.R. § 164.304.

158. ADG breached its duties to Plaintiff and Class Members under the FTCA and
HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security
practices to safeguard Plaintiff's and Class Members' Private Information.

24 159. Specifically, ADG breached its duties by failing to employ industry-standard
25 cybersecurity measures in order to comply with the FTCA, including but not limited to proper
26 segregation, access controls, password protection, encryption, intrusion detection, secure
27 destruction of unnecessary data, and penetration testing.

1 160. The FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as
2 interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures
3 to protect PII and PHI (such as the Private Information compromised in the Data Breach). The
4 FTC rulings and publications described above, together with the industry-standard cybersecurity
5 measures set forth herein, form part of the basis of ADG’s duty in this regard.

6 161. ADG also violated the FTCA and HIPAA by failing to use reasonable measures to
7 protect the Private Information of Plaintiff and the Class and by not complying with applicable
8 industry standards, as described herein.

9 162. It was reasonably foreseeable, particularly given the growing number of data
10 breaches of Private Information, that the failure to reasonably protect and secure Plaintiff’s and
11 Class Members’ Private Information in compliance with applicable laws would result in an
12 unauthorized third-party gaining access to ADG’s networks, databases, and computers that stored
13 Plaintiff’s and Class Members’ unencrypted Private Information.

14 163. Plaintiff and Class Members are within the class of persons that the FTCA and
15 HIPAA are intended to protect, and ADG’s failure to comply with both constitutes negligence per
16 se.

17 164. Plaintiff’s and Class Members’ Private Information constitutes personal property
18 that was stolen due to ADG’s negligence, resulting in harm, injury, and damages to Plaintiff and
19 Class Members.

20 165. As a direct and proximate result of ADG’s negligence per se, Plaintiff and the Class
21 have suffered, and continue to suffer, injuries and damages arising from the unauthorized access
22 of their Private Information, including but not limited to damages from the actual misuse of their
23 Private Information and the lost time and effort to mitigate the actual and potential impact of the
24 Data Breach on their lives.

25 166. As a direct and proximate result of ADG’s negligent conduct, Plaintiff and Class
26 Members have suffered injury and are entitled to compensatory and consequential damages in an
27 amount to be proven at trial.

28

1 167. In addition to monetary relief, Plaintiff and Class Members are also entitled to
2 injunctive relief requiring ADG to, *inter alia*, strengthen its data security systems and monitoring
3 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
4 identity theft insurance to Plaintiff and Class Members.

COUNT III

BREACH OF CONTRACT

7 168. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
8 set forth herein.

9 169. Plaintiff and Class Members entered into a valid and enforceable contract through
10 which they paid money to ADG in exchange for services. That contract included promises by
11 Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private
12 Information.

13 170. ADG's Privacy Policy memorialized the rights and obligations of ADG and its
14 patients. This document was provided to Plaintiff and Class Members in a manner in which it
15 became part of the agreement for services.

16 171. In the Privacy Policy, ADG commits to protecting the privacy and security of
17 private information and promises to never share Plaintiff's and Class Members' Private
18 Information except under certain limited circumstances.

19 172. Plaintiff and Class Members fully performed their obligations under their contracts
20 with ADG.

173. However, ADG did not secure, safeguard, and/or keep private Plaintiff's and Class
Members' Private Information, and therefore ADG breached its contracts with Plaintiff and Class
Members.

174. ADG allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class
25 Members' Private Information without permission. Therefore, ADG breached the Privacy Policy
26 with Plaintiff and Class Members.

1 175. ADG's failure to satisfy its confidentiality and privacy obligations, specifically
2 those arising under the FTCA, HIPAA, and applicable industry standards, resulted in ADG
3 providing services to Plaintiff and Class Members that were of a diminished value.

4 176. As a result, Plaintiff and Class Members have been harmed, damaged, and/or
5 injured as described herein, including in Defendant's failure to fully perform its part of the bargain
6 with Plaintiff and Class Members.

7 177. As a direct and proximate result of ADG's conduct, Plaintiff and Class Members
8 suffered and will continue to suffer damages in an amount to be proven at trial.

9 178. In addition to monetary relief, Plaintiff and Class Members are also entitled to
10 injunctive relief requiring ADG to, *inter alia*, strengthen its data security systems and monitoring
11 procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and
12 identity theft insurance to Plaintiff and Class Members.

COUNT IV

BREACH OF IMPLIED CONTRACT

15 179. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
16 set forth herein.

17 || 180. This Count is pleaded in the alternative to Count III above.

18 181. ADG provides dental and related services to Plaintiff and Class Members. Plaintiff
19 and Class Members formed an implied contract with Defendant regarding the provision of those
20 services through their collective conduct, including by Plaintiff and Class Members paying for
21 services and/or entrusting their valuable Private Information to Defendant in exchange for such
22 services.

182. Through Defendant's sale of services to Plaintiff and Class Members, it knew or
should have known that it must protect Plaintiff's and Class Members' confidential Private
Information in accordance with its policies, practices, and applicable law.

183. As consideration, Plaintiff and Class Members paid money to ADG and/or turned
over valuable Private Information to ADG. Accordingly, Plaintiff and Class Members bargained
with ADG to securely maintain and store their Private Information.

1 184. ADG accepted payment and/or possession of Plaintiff's and Class Members'
2 Private Information for the purpose of providing services to Plaintiff and Class Members.

3 185. In paying Defendant and/or providing their valuable Private Information to
4 Defendant in exchange for Defendant's services, Plaintiff and Class Members intended and
5 understood that ADG would adequately safeguard the Private Information as part of those services.

6 186. Defendant's implied promises to Plaintiff and Class Members include, but are not
7 limited to: (1) taking steps to ensure that anyone who is granted access to Private Information also
8 protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that
9 is placed in the control of its employees is restricted and limited to achieve an authorized business
10 purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and
11 implementing appropriate retention policies to protect the Private Information against criminal
12 data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor
13 authentication for access; (7) complying with HIPAA standards to make sure that Plaintiff's and
14 Class Members' PHI would remain protected; and (8) taking other steps to protect against
15 foreseeable data breaches.

16 187. Plaintiff and Class Members would not have entrusted their Private Information to
17 ADG in the absence of such an implied contract.

18 188. Had ADG disclosed to Plaintiff and the Class that it did not have adequate computer
19 systems and security practices to secure sensitive data, Plaintiff and Class Members would not
20 have provided their Private Information to ADG.

21 189. As a provider of dental health services, ADG recognized (or should have
22 recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must
23 be protected, and that this protection was of material importance as part of the bargain with
24 Plaintiff and the other Class Members.

25 190. ADG violated these implied contracts by failing to employ reasonable and adequate
26 security measures to secure Plaintiff's and Class Members' Private Information. ADG further
27 breached these implied contracts by failing to comply with its promise to abide by HIPAA.
28

1 191. Additionally, ADG breached the implied contracts with Plaintiff and Class
2 Members by failing to ensure the confidentiality and integrity of electronic protected health
3 information it created, received, maintained, and transmitted, in violation of 45 CFR
4 164.306(a)(1).

5 192. ADG also breached the implied contracts with Plaintiff and Class Members by
6 failing to implement technical policies and procedures for electronic systems that maintain
7 electronic PHI to allow access only to those persons or software programs that have been granted
8 access rights, in violation of 45 CFR 164.312(a)(1).

9 193. ADG further breached the implied contracts with Plaintiff and Class Members by
10 failing to implement policies and procedures to prevent, detect, contain, and correct security
11 violations, in violation of 45 CFR 164.308(a)(1).

12 194. ADG further breached the implied contracts with Plaintiff and Class Members by
13 failing to identify and respond to suspected or known security incidents; mitigate, to the extent
14 practicable, harmful effects of security incidents that are known to the covered entity, in violation
15 of 45 CFR 164.308(a)(6)(ii).

16 195. ADG further breached the implied contracts with Plaintiff and Class Members by
17 failing to protect against any reasonably anticipated threats or hazards to the security or integrity
18 of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

19 196. ADG further breached the implied contracts with Plaintiff and Class Members by
20 failing to protect against any reasonably anticipated uses or disclosures of electronic protected
21 health information that are not permitted under the privacy rules regarding individually identifiable
22 health information, in violation of 45 CFR 164.306(a)(3).

23 197. ADG further breached the implied contracts with Plaintiff and Class Members by
24 failing to ensure compliance with the HIPAA security standard rules by its workforce violations,
25 in violation of 45 CFR 164.306(a)(94).

26 198. ADG further breached the implied contracts with Plaintiff and Class Members by
27 impermissibly and improperly using and disclosing protected health information that is and
28 remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

1 199. ADG further breached the implied contracts with Plaintiff and Class Members by
2 failing to design, implement, and enforce policies and procedures establishing physical
3 administrative safeguards to reasonably safeguard protected health information, in violation of 45
4 CFR 164.530(c).

5 200. ADG further breached the implied contracts with Plaintiff and Class Members by
6 otherwise failing to safeguard Plaintiff's and Class Members' PHI.

7 201. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*,
8 to provide payment and/or accurate and complete Private Information to ADG in exchange for
9 ADG's agreement to, *inter alia*, provide services that included protection of their highly sensitive
10 Private Information.

11 202. Plaintiff and Class Members have been damaged by ADG's conduct, including the
12 harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V

UNJUST ENRICHMENT

15 203. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
16 set forth herein.

204. This Count is pleaded in the alternative to Counts III and IV above.

18 205. Plaintiff and Class Members conferred a benefit on ADG by turning over their
19 Private Information to Defendant and by paying for services that should have included
20 cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not
21 receive such protection.

22 206. Upon information and belief, ADG funds its data security measures entirely from
23 its general revenue, including from payments made to it by Plaintiff and Class Members.

24 207. As such, a portion of the payments made by Plaintiff and Class Members is to be
25 used to provide a reasonable and adequate level of data security that is in compliance with
26 applicable state and federal regulations and industry standards, and the amount of the portion of
27 each payment made that is allocated to data security is known to ADG.

1 208. ADG has retained the benefits of its unlawful conduct, including the amounts of
2 payment received from Plaintiff and Class Members that should have been used for adequate
3 cybersecurity practices that it failed to provide.

4 209. ADG knew that Plaintiff and Class Members conferred a benefit upon it, which
5 ADG accepted. ADG profited from these transactions and used the Private Information of Plaintiff
6 and Class Members for business purposes, while failing to use the payments it received for
7 adequate data security measures that would have secured Plaintiff's and Class Members' Private
8 Information and prevented the Data Breach.

9 210. If Plaintiff and Class Members had known that ADG had not adequately secured
10 their Private Information, they would not have agreed to provide such Private Information to
11 Defendant.

12 211. Due to ADG's conduct alleged herein, it would be unjust and inequitable under the
13 circumstances for ADG to be permitted to retain the benefit of its wrongful conduct.

14 212. As a direct and proximate result of ADG's conduct, Plaintiff and Class Members
15 have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not
16 limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control how their
17 Private Information is used; (iii) the compromise, publication, and/or theft of their Private
18 Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery
19 from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs
20 associated with effort expended and the loss of productivity addressing and attempting to mitigate
21 the actual and future consequences of the Data Breach, including but not limited to efforts spent
22 researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk
23 to their Private Information, which remains in ADG's possession and is subject to further
24 unauthorized disclosures so long as ADG fails to undertake appropriate and adequate measures to
25 protect Private Information in its continued possession; and (vii) future costs in terms of time,
26 effort, and money that will be expended to prevent, detect, contest, and repair the impact of the
27 Private Information compromised as a result of the Data Breach for the remainder of the lives of
28 Plaintiff and Class Members.

1 213. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages
2 from ADG and/or an order proportionally disgorging all profits, benefits, and other compensation
3 obtained by ADG from its wrongful conduct. This can be accomplished by establishing a
4 constructive trust from which the Plaintiff and Class Members may seek restitution or
5 compensation.

6 214. Plaintiff and Class Members may not have an adequate remedy at law against ADG,
7 and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to,
8 other claims pleaded herein.

COUNT VI

BREACH OF FIDUCIARY DUTY

11 215. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
12 set forth herein.

13 216. In light of the special relationship between ADG and its patients, whereby ADG
14 became a guardian of Plaintiff's and Class Members' Private Information (including highly
15 sensitive, confidential, personal, and other PHI) ADG was a fiduciary, created by its undertaking
16 and guardianship of the Private Information, to act primarily for the benefit of its patients,
17 including Plaintiff and Class Members. This benefit included (1) the safeguarding of Plaintiff's
18 and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of the
19 Data Breach; and (3) maintaining complete and accurate records of what and where ADG's
20 patients' Private Information was and is stored.

21 217. ADG had a fiduciary duty to act for the benefit of Plaintiff and the Class upon
22 matters within the scope of its patients' relationship, in particular to keep the Private Information
23 secure.

24 218. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
25 diligently investigate the Data Breach to determine the number of Class Members affected and
26 notify them within a reasonable and practicable period of time.

27 219. ADG breached its fiduciary duties to Plaintiff and the Class by failing to protect
28 their Private Information.

1 220. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
2 ensure the confidentiality and integrity of electronic PHI ADG created, received, maintained, and
3 transmitted, in violation of 45 CFR 164.306(a)(1).

4 221. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
5 implement technical policies and procedures for electronic information systems that maintain
6 electronic PHI to allow access only to those persons or software programs that have been granted
7 access rights, in violation of 45 CFR 164.312(a)(1).

8 222. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
9 implement policies and procedures to prevent, detect, contain, and correct security violations, in
10 violation of 45 CFR 164.308(a)(1).

11 223. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
12 identify and respond to suspected or known security incidents; mitigate, to the extent practicable,
13 harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR
14 164.308(a)(6)(ii).

15 224. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
16 protect against any reasonably-anticipated threats or hazards to the security or integrity of
17 electronic PHI, in violation of 45 CFR 164.306(a)(2).

18 225. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
19 protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not
20 permitted under the privacy rules regarding individually identifiable health information, in
21 violation of 45 CFR 164.306(a)(3).

22 226. ADG breached its fiduciary duties to Plaintiff and Class Members by failing to
23 ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45
24 CFR 164.306(a)(94).

25 227. ADG breached its fiduciary duties to Plaintiff and Class Members by impermissibly
26 and improperly using and disclosing PHI that is and remains accessible to unauthorized persons,
27 in violation of 45 CFR 164.502, *et seq.*

1 228. As a direct and proximate result of ADG's breaches of its fiduciary duties, Plaintiff
2 and Class Members have suffered and will continue to suffer the harms and injuries alleged herein,
3 as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic
4 losses.

COUNT VII

BREACH OF CONFIDENCE

7 229. Plaintiff restates and incorporates by reference all preceding paragraphs as if fully
8 set forth herein.

9 230. Plaintiff and Class Members have an interest, both equitable and legal, in the
10 Private Information about them that was conveyed to, collected by, and maintained by ADG and
11 ultimately accessed and acquired in the Data Breach.

12 231. As a healthcare provider, ADG has a special, fiduciary relationship with its patients,
13 including Plaintiff and Class Members. Because of that special relationship, ADG was provided
14 with and stored Plaintiff's and Class Members' Private Information and had a duty to maintain the
15 Private Information in confidence.

16 232. Patients like Plaintiff and Class Members have a privacy interest in personal
17 medical and other matters, and ADG had a duty not to disclose such matters concerning its patients.

18 233. As a result of the parties' relationship, ADG had possession and knowledge of
19 highly sensitive and confidential Private Information belonging to Plaintiff and Class Members,
20 information that was not generally known.

21 234. Plaintiff and Class Members did not consent nor authorize Defendant to release or
22 disclose their Private Information to an unknown criminal actor.

23 235. ADG breached its duty of confidence owed to Plaintiff and Class Members by,
24 among other things: (a) mismanaging its system and failing to identify reasonably foreseeable
25 internal and external risks to the security, confidentiality, and integrity of patient information that
26 resulted in the unauthorized access and compromise of Plaintiff's and Class Members' Private
27 Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards
28 in place to control these risks; (c) failing to design and implement adequate information safeguards

1 to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards'
2 key controls, systems, and procedures; (e) failing to evaluate and adjust its information security
3 program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the
4 time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies
5 and practices published to its patients; and (h) making an unauthorized and unjustified disclosure
6 and release of Plaintiff's and Class members' Private Information to a criminal third party.

7 236. But for ADG's wrongful breach of its duty of confidence owed to Plaintiff and
8 Class Members, their Private Information would not have been compromised.

9 237. As a direct and proximate result of ADG's wrongful breach of its duty of
10 confidence, Plaintiff and Class Members have suffered and will continue to suffer the injuries
11 alleged herein.

12 238. It would be inequitable for ADG to retain the benefit of controlling and maintaining
13 Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

14 239. Plaintiff and Class Members are entitled to damages, including compensatory,
15 punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven
16 at trial.

COUNT VIII

DECLARATORY AND INJUNCTIVE RELIEF, 28 U.S.C. § 2201

19 240. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. §
20 2201.

21 241. Defendant owes a duty of care to Plaintiff and Class Members that required them
22 to adequately secure their Private Information.

23 242. Defendant still possess Plaintiff's and Class Members' Private Information, yet
24 does not adequately protect PII against the threat of another data breach.

243. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff
and Class Members.

27 244. Actual harm has arisen in the wake of the Data Breach regarding Defendant's
28 obligations and duties of care to provide security measures to Plaintiff and Class Members.

1 Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure
2 of their Private Information and Defendant's ongoing failure to address the security failings that
3 led to such exposure.

4 245. There is no reason to believe that Defendant's employee training and security
5 measures are any more adequate now than they were before the Data Breach.

6 246. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security
7 measures do not comply with its contractual obligations and duties of care to provide adequate
8 data security, and (2) that to comply with its obligations and duties of care, Defendant must
9 implement and maintain reasonable security measures, including, but not limited to, being ordered
10 as follows:

- 11 a. prohibiting Defendant from engaging in the wrongful and unlawful acts described
12 herein;
- 13 b. ordering that Defendant engage internal security personnel to conduct testing,
14 including audits on Defendant's systems, on a periodic basis, and ordering
15 Defendant to promptly correct any problems or issues detected by such third-party
16 security auditors;
- 17 c. requiring Defendant to protect, including through encryption, all data collected
18 through the course of its business in accordance with all applicable regulations,
19 industry standards, and federal, state, or local laws;
- 20 d. ordering that Defendant engage third-party security auditors and internal personnel
21 to run automated security monitoring;
- 22 e. ordering that Defendant audit, test, and train security personnel and employees
23 regarding any new or modified data security policies and procedures;
- 24 f. ordering that Defendant purge, delete, and destroy, in a reasonably secure manner,
25 any Private Information not necessary for provision of services;
- 26 g. ordering that Defendant conduct regular database scanning and security checks;
- 27 h. prohibiting Defendant from maintaining Private Information of Plaintiff and Class
28 Members on a cloud-based database;

- i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- j. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Private Information;
- k. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- l. requiring Defendant to meaningfully educate all class members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- m. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and
- n. such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class described above, seeks the following relief:

- a. Certifying the class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

- 1 b. Judgment in favor of Plaintiff and Class Members awarding them appropriate
- 2 monetary relief, including actual damages, statutory damages, equitable relief,
- 3 restitution, disgorgement, and statutory costs;
- 4 c. An order providing injunctive and other equitable relief as necessary to protect the
- 5 interests of the Class as requested herein;
- 6 d. An order instructing ADG to purchase or provide funds for lifetime credit
- 7 monitoring and identity theft insurance to Plaintiff and Class Members;
- 8 e. An order requiring ADG to pay the costs involved in notifying Class Members
- 9 about the judgment and administering the claims process;
- 10 f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment
- 11 and post-judgment interest, reasonable attorneys' fees, costs, and expenses as
- 12 allowable by law; and
- 13 g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

247. Pursuant to Federal Rule of Civil Procedure 38 and the seventh amendment to the
 Constitution of the United States of America and the Constitution of the State of Nevada,
 Plaintiff is entitled to, and demands a trial by jury.

DATED: June 4, 2025.

19 Respectfully submitted,

20 /s/ Gerardo Avalos

21 George Haines, Esq.

22 Gerardo Avalos, Esq.

23 **FREEDOM LAW FIRM**

24 8985 S. Eastern Avenue, Suite 100

25 Las Vegas, NV 89123

26 Andrew W. Ferich, Esq. (*pro hac vice* forthcoming)

27 **AHDOOT & WOLFSON, PC**

28 201 King of Prussia Road, Suite 650

Radnor, PA 19087

Telephone: (310) 474-9111

Facsimile: (310) 474-8585

aferich@ahdootwolfson.com

1 Alyssa Brown, Esq. (*pro hac vice* forthcoming)
2 **AHDOOT & WOLFSON, PC**
3 2600 W. Olive Avenue, Suite 500
4 Burbank, CA 91505
5 Telephone: (310) 474-9111
Facsimile: (310) 474-8585
abrown@ahdootwolfson.com

6 *Counsel for Plaintiff and the Proposed Class*

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28